瞭解會議伺服器上的呼叫路由邏輯

目錄

簡介

本文檔介紹思科Meeting Server (CMS)（以前稱為Acano產品）的呼叫路由邏輯，該邏輯分為幾個呼叫路由表。本文檔介紹呼叫透過這些呼叫路由表可以採取的不同階段和方案。

必要條件

需求

思科建議您瞭解以下主題：

- 思科會議伺服器呼叫網橋元件。

採用元件

本文檔中的資訊基於2.3.x版的Cisco Meeting Server。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

思科Meeting Server (CMS)的呼叫路由邏輯是什麼？

CMS上的呼叫路由涉及幾個呼叫路由不同的表。透過可下載的流程圖，您可以遵循到達CMS的每個呼叫的呼叫路由邏輯。這適用於所有型別的呼叫：思科會議應用（CMA -厚客戶端或WebRTC）、標準會話發起協定(SIP)呼叫或Microsoft SIP呼叫（除非另有指定）。

注意：唯一的例外是CMS發起的呼叫(CMS直接用於TelePresence Management Suite (TMS)計畫的出站呼叫或CMA客戶端呼叫)，呼叫轉發表被繞過。

這是CMS內呼叫路由過程的順序：

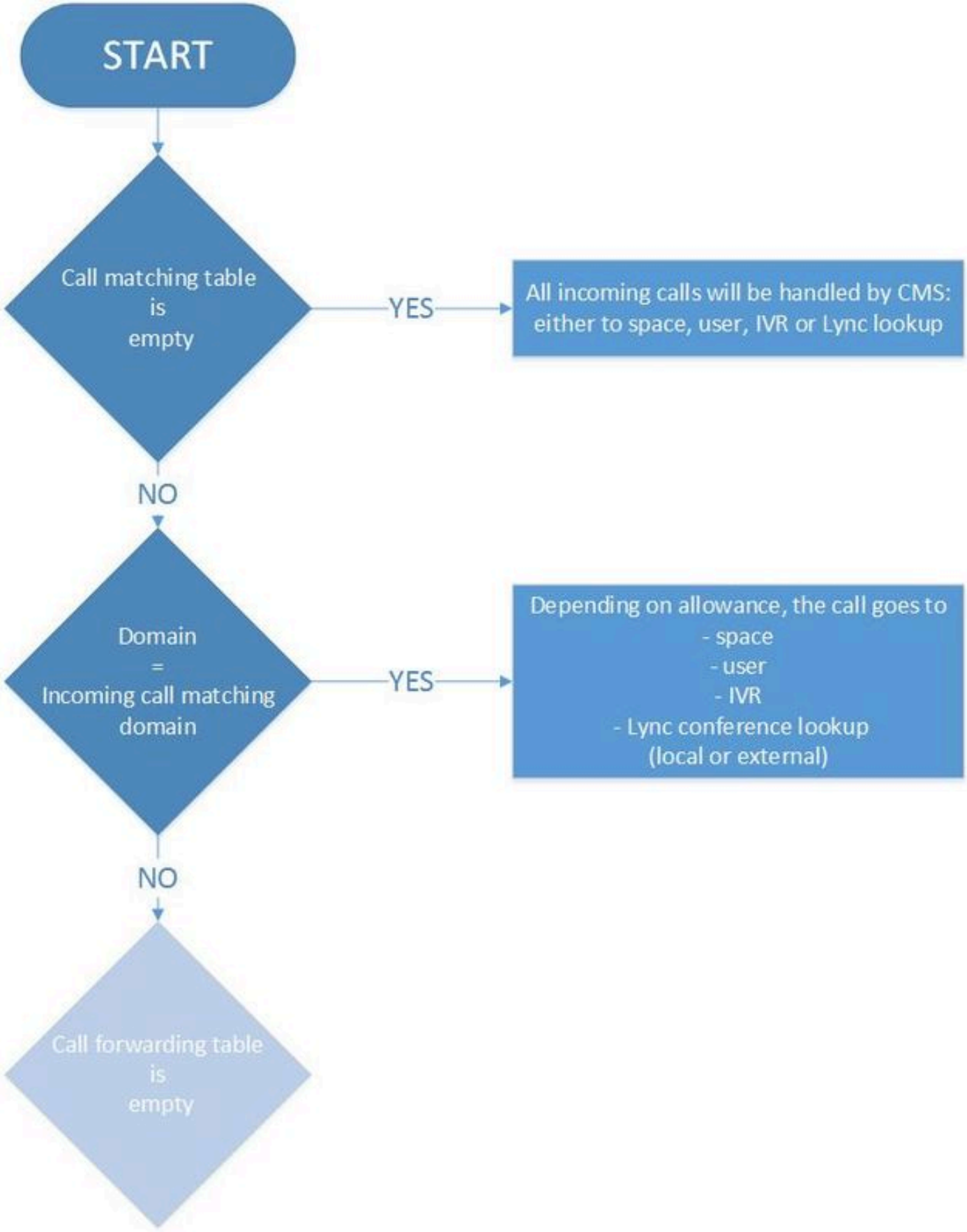
1. 來電匹配表
2. 來電轉接表
3. 出站呼叫表

每個表格將在本文檔後面部分進行更詳細的介紹，其中包括僅顯示相關部分的影象。

注意：CMS僅基於域路由執行呼叫路由，因此基於統一資源識別符號(URI)的右側(RHS)。沒有基於URI左側(LHS)的呼叫路由功能，就像在具有目錄號碼路由（路由模式）的Cisco Unified Communications Manager (CUCM)中一樣。

備註：每個表格都是由優先順序屬性所設定的排序清單。優先順序越高，表示它會先嘗試匹配。如果不匹配，則繼續清單中的下一個規則。作為一般經驗法則，給予較一般規則（如與任何領域匹配的*）比較具體規則較低的優先順序。這樣，系統會先處理特定規則，您可能會退回到更一般的規則。

步驟 1.來電匹配表

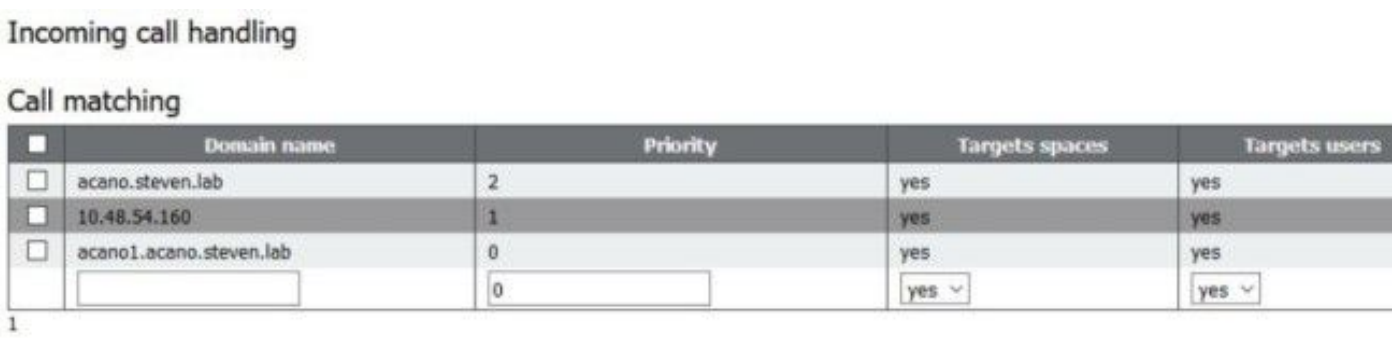


這是CMS確定入站呼叫是否發往思科Meeting Server本身，並且需要在該伺服器上進一步處理，或者該呼叫是否發往另一個系統(其中CMS是處理呼叫的代理並處理媒體和信令（例如，到標準SIP終端的Skype網關呼叫，反之亦然）的第一步。

它檢查傳入URI的域部分是否與傳入的匹配表匹配。如果匹配，則它能夠根據此撥號方案規則的配置將呼叫路由到空間、使用者、IVR或執行Lync會議查詢（內部或外部）。該表不允許使用萬用字元域，它要求完全匹配。

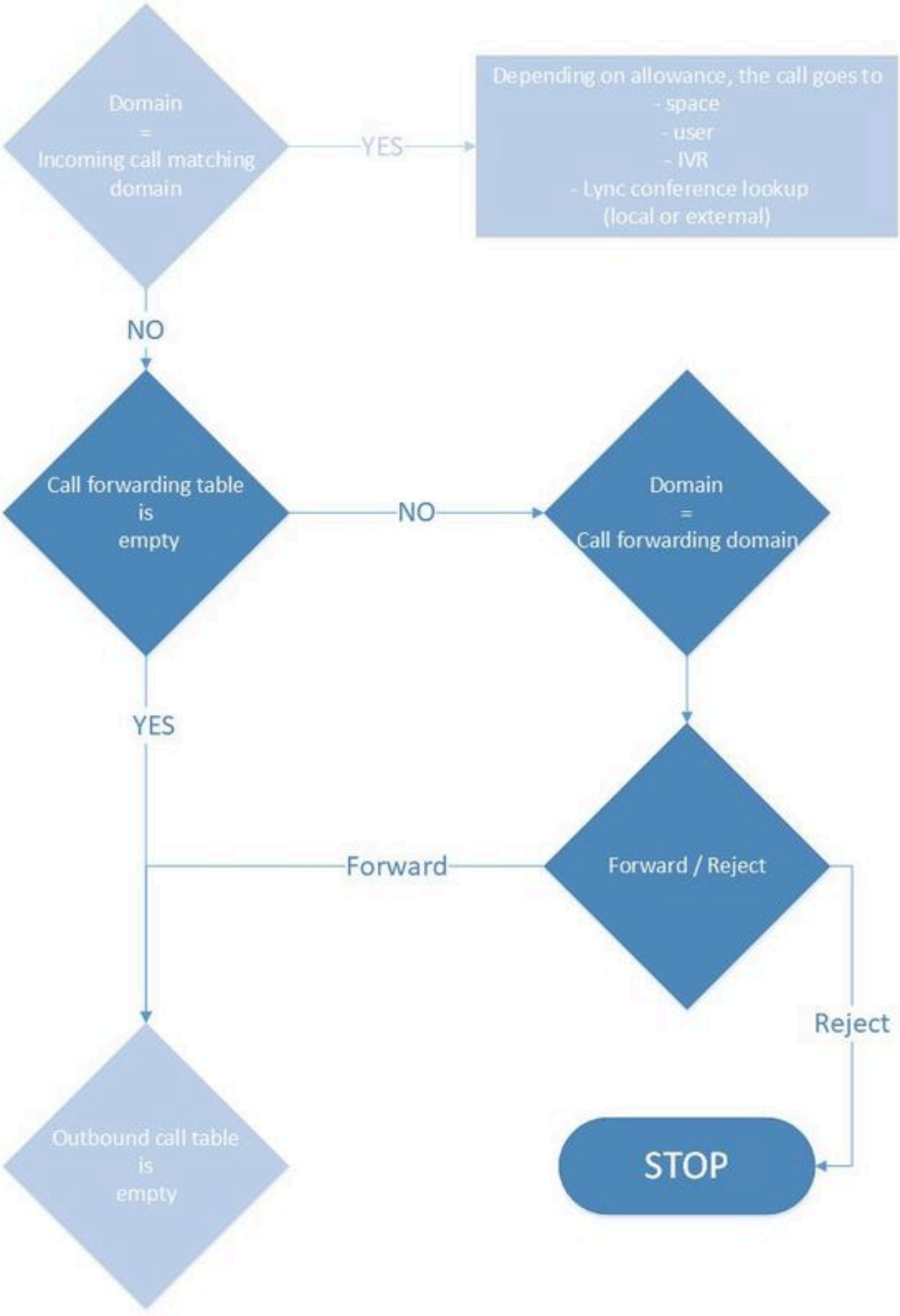
注意：如果未配置任何傳入呼叫匹配域，則CMS會接受來自SIP的所有傳入URI或來自Lync的呼入URI，這些呼入呼叫均位於Callbridge上。對於CMA客戶端（WebRTC或厚客戶端），雖然它接受呼叫，但不會自動路由到正確的空間或使用者。因此，在這種情況下，當您使用CMA客戶端撥號到空間或使用者時，在正確的域中輸入資訊非常重要。

例如，圖中顯示了一個呼叫匹配表(它僅顯示了目標空間和目標使用者選項以提供簡潔性)：



此處，域設定為acano.steven.lab，客戶端通常撥打該域。但是，它還允許臨時呼叫或來自CUCM（或Expressway搜尋規則）的特定SIP路由模式，這些模式僅透過表中的第一和第二後退規則來定位特定的Callbridge（如果是集群），該規則匹配Callbridge的IP地址（本例中為10.48.54.160）或Callbridge的完全限定域名(FQDN)（在本例中為acano1.acano.steven.lab）。

步驟 2.來電轉接表



如果呼叫沒有遇到來電匹配表上的任何規則，或者沒有匹配規則使呼叫繼續（例如，使用者撥打了

參與者之間的網關的狀態，例如沒有任何呼叫轉發規則。假設傳入呼叫的域在傳入呼叫匹配表中不匹配，或者域匹配，但在空間、使用者或IVR（或Skype會議）上沒有匹配，則不會針對出站呼叫表轉發呼叫。

注意：這種情況在CMA客戶端（胖客戶端和WebRTC）中確實會發生，因為它們能夠進行出站呼叫（*3.0中的Web App無法進行出站呼叫，而是由由Callbridge撥出的CMS空間進行的呼叫）。同樣，透過API（例如，在TMS計畫會議中）進行CMS上的出站呼叫也可以正常工作。一般來說，從CMS本身（直接或透過CMA）發起的呼叫不能遵循呼叫轉發邏輯。

例如，當CMS用作SIP和Skype呼叫的網關時，您可以在事件日誌中看到突出顯示的forwarding消息。在此之前，您可以看到來電呼叫和隨後的去話呼叫。

<#root>

```
2018-10-04  06:36:24.612  Info      call 788:
```

incoming

```
SIP call from "sip:1060@10.48.36.215" to local URI "sip:stejanss@any.com"
2018-10-04  06:36:24.624  Info
```

forwarding call

```
 to 'sip:stejanss@any.com' to 'stejanss@any.com'
2018-10-04  06:36:24.625  Info      call 789:
```

outgoing

```
SIP call to "stejanss@any.com"
```

如果轉發表沒有任何規則或拒絕規則，則事件日誌不會明確顯示此規則。它只是通知您SIP呼叫不匹配（任何空間、使用者、IVR或Lync會議），並且您錯過轉發規則（或將其設定為拒絕）以轉到outbound rules部分。

<#root>

```
2018-10-04  06:47:12.482  Info      call 790:
```

incoming

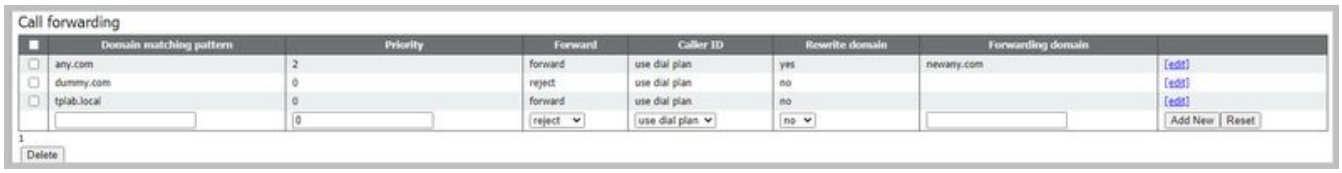
```
SIP call from "sip:1060@10.48.36.215" to local URI "sip:stejanss@any.com"
2018-10-04  06:47:12.495  Info      call 790: ending; local teardown, destination URI not matched - not
```

對於透過TMS計畫會議發起的CMA客戶端呼叫或CMS的出站呼叫，事件日誌中沒有呼入呼叫。呼叫會立即轉到出站撥號方案表，並且呼叫轉發表不會處理該呼叫。

在呼叫轉發表中，還有另外兩個配置選項：重寫域和呼叫方ID。

重寫域

此選項允許您將入站呼叫的域重寫為另一個域，並更改SIP消息的SIP請求URI的域部分以及到信頭
。



例如，根據此影象上的配置，此處將顯示包含域any.com的入站呼叫的事件日誌（啟用SIP跟蹤
），但是沒有在傳入呼叫匹配表（在空間、使用者、IVR或Skype會議上）中匹配：

<#root>

```
2018-10-04  07:02:24.818  Info      SIP trace: connection 0: incoming SIP TCP data from 10.48.36.215:564
2018-10-04  07:02:24.818  Info      SIP trace:

INVITE

 sip:stejanss@

any.com

 SIP/2.0
2018-10-04  07:02:24.818  Info      SIP trace: Via: SIP/2.0/TCP 10.48.36.215:5060;branch=z9hG4bK53e4c4ce
2018-10-04  07:02:24.818  Info      SIP trace: From: "EX60 Steven" <sip:1060@steven.lab>;tag=742103~ee54
2018-10-04  07:02:24.818  Info      SIP trace:

To:

 <sip:stejanss@

any.com

>
..
2018-10-04  07:02:24.822  Info      call 797:

incoming

 SIP call from "sip:1060@10.48.36.215" to local URI "sip:stejanss@

any.com

"
2018-10-04  07:02:24.834  Info

forwarding

 call to 'sip:stejanss@

any.com

' to 'stejanss@

newany.com

'
2018-10-04  07:02:24.835  Info      call 798:

outgoing

 SIP call to "stejanss@
```

```
newany.com

"
..
2018-10-04  07:02:24.838  Info      SIP trace: connection 19: outgoing SIP TCP data to 10.48.36.215:5060
2018-10-04  07:02:24.838  Info      SIP trace:

INVITE

 sip:stejanss@

newany.com

 SIP/2.0
2018-10-04  07:02:24.838  Info      SIP trace: Via: SIP/2.0/TCP 10.48.80.71:5060;branch=z9hG4bKefc98b81a
2018-10-04  07:02:24.839  Info      SIP trace: Call-ID: 18644f28-e998-4032-a7df-75325e9d11b0
2018-10-04  07:02:24.839  Info      SIP trace: CSeq: 659590315 INVITE
2018-10-04  07:02:24.839  Info      SIP trace: Max-Forwards: 70
2018-10-04  07:02:24.839  Info      SIP trace: Contact: <sip:1060@10.48.80.71;transport=tcp>
2018-10-04  07:02:24.839  Info      SIP trace:

To

: <sip:stejanss@

newany.com

>
2018-10-04  07:02:24.839  Info      SIP trace: From: "EX60 Steven" <sip:1060@steven.lab>;tag=2aa2a49bba2
```

在此轉接呼叫行中，它顯示發生的修改。如果您未啟用SIP跟蹤，仍然會顯示對any.com到newany.com的修改。

此域重寫的最常見用法是預先Lync與CMS群集的整合，其中建議將出站規則中的「聯絡人」報頭和「發件人」報頭設定為Lync/Skype到Callbridge特定的完全限定域名(FQDN)。這是因為以下路由規則：

- Skype會在通話方塊中傳送新的交易（例如，邀請- 200 OK之後的ACK）至其從CMS收到的200 OK中指定的連絡人標頭。對於從Skype到CMS的傳入連線，Skype會先傳送一個交涉SIP訊息，在To標頭中包含ms-fe標頭，該標頭會指定如何在INVITE的200 OK回覆中填寫（因為它使用相同的TCP通道）
- Skype將新對話方塊（如內容共用，因為它是單獨的呼叫，如果呼叫未接則發回呼叫）傳送到原始INVITE的From標頭

在重寫域時，它與Lync呼叫的回撥相關。未接的INVITE的From報頭指向呼叫來自的特定Callbridge。然後，Lync會傳送一個新請求(INVITE)，其中包含與Callbridge FQDN匹配的SIP請求URI。 然後透過這些重寫規則將其轉換為SIP域。 呼叫轉發後，會使用出站規則到達SIP終端註冊的CUCM或Expressway-C。

來電者ID

這裡有兩個選項可以在轉發規則上設定。此設定設定為pass through，然後不對出站INVITE的From報頭進行修改，或者設定為use dial plan，以便系統根據出站規則修改From報頭。此設定與域是否重寫無關，因為僅涉及SIP請求URI以及出站INVITE的To報頭。

例如，與以前進行的呼叫相同，但現在有一個到newany.com的出站撥號方案規則（如在重寫傳入呼叫轉發表之後）設定為一個Lync型別呼叫（例如，Ms-Conversation-ID作為額外SIP報頭）。適在地填寫本地源域（和本地聯絡域）以指向先前所示的Lync呼叫的Callbridge FQDN。然後，這將反映出站SIP INVITE From和Contact報頭的更改。 如圖所示，它們會以相同的值填充，並可以根據需要單獨選擇。

Outbound calls

Filter Submit Query

■	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority
□	steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	5
□	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4

<#root>

```
2018-10-12  09:09:24.488  Info      SIP trace: connection 28: incoming SIP TCP data from 10.48.36.215:44
2018-10-12  09:09:24.489  Info      SIP trace: INVITE sip:stejanss@any.com SIP/2.0
2018-10-12  09:09:24.489  Info      SIP trace: Via: SIP/2.0/TCP 10.48.36.215:5060;branch=z9hG4bKf4a230ec
2018-10-12  09:09:24.489  Info      SIP trace:
```

From

```
: "EX60 Steven" <sip:1060@
```

steven.lab

```
>;tag=118288~ee545a46-516a-4de6-87d7-7b1f5a5b848a-32900729
2018-10-12  09:09:24.489  Info      SIP trace: To: <sip:stejanss@any.com>
2018-10-12  09:09:24.489  Info      SIP trace: Call-ID: 81e67f80-bc0164c4-f2c6-d724300a@10.48.36.215

2018-10-12  09:09:24.494  Info      call 803:
```

incoming

```
 SIP call from "sip:1060@10.48.36.215" to local URI "sip:stejanss@any.com"
2018-10-12  09:09:24.506  Info
```

forwarding call

```
 to 'sip:stejanss@any.com' to 'stejanss@newany.com'
2018-10-12  09:09:24.507  Info      call 804:
```

outgoing

```
 SIP call to "stejanss@newany.com" (Lync)

2018-10-12  09:09:24.507  Info      SIP trace: connection 33: allocated for outgoing connection to 10.48
2018-10-12  09:09:24.508  Info      SIP trace: connection 33: outgoing connection successful, 10.48.80.7
2018-10-12  09:09:24.510  Info      SIP trace: connection 33: outgoing SIP TCP data to 10.48.36.46:5060
2018-10-12  09:09:24.510  Info      SIP trace: INVITE sip:stejanss@newany.com SIP/2.0
2018-10-12  09:09:24.510  Info      SIP trace: Via: SIP/2.0/TCP 10.48.80.71:5060;branch=z9hG4bK15bdde97a
2018-10-12  09:09:24.510  Info      SIP trace: Call-ID: c366ddaf-e602-4fa5-b1d6-2e16ec08534a
2018-10-12  09:09:24.510  Info      SIP trace: CSeq: 1498747095 INVITE
2018-10-12  09:09:24.510  Info      SIP trace: Max-Forwards: 70
2018-10-12  09:09:24.510  Info      SIP trace:
```

Contact

```
: <sip:1060@
```

callbridgefqdn.any.com

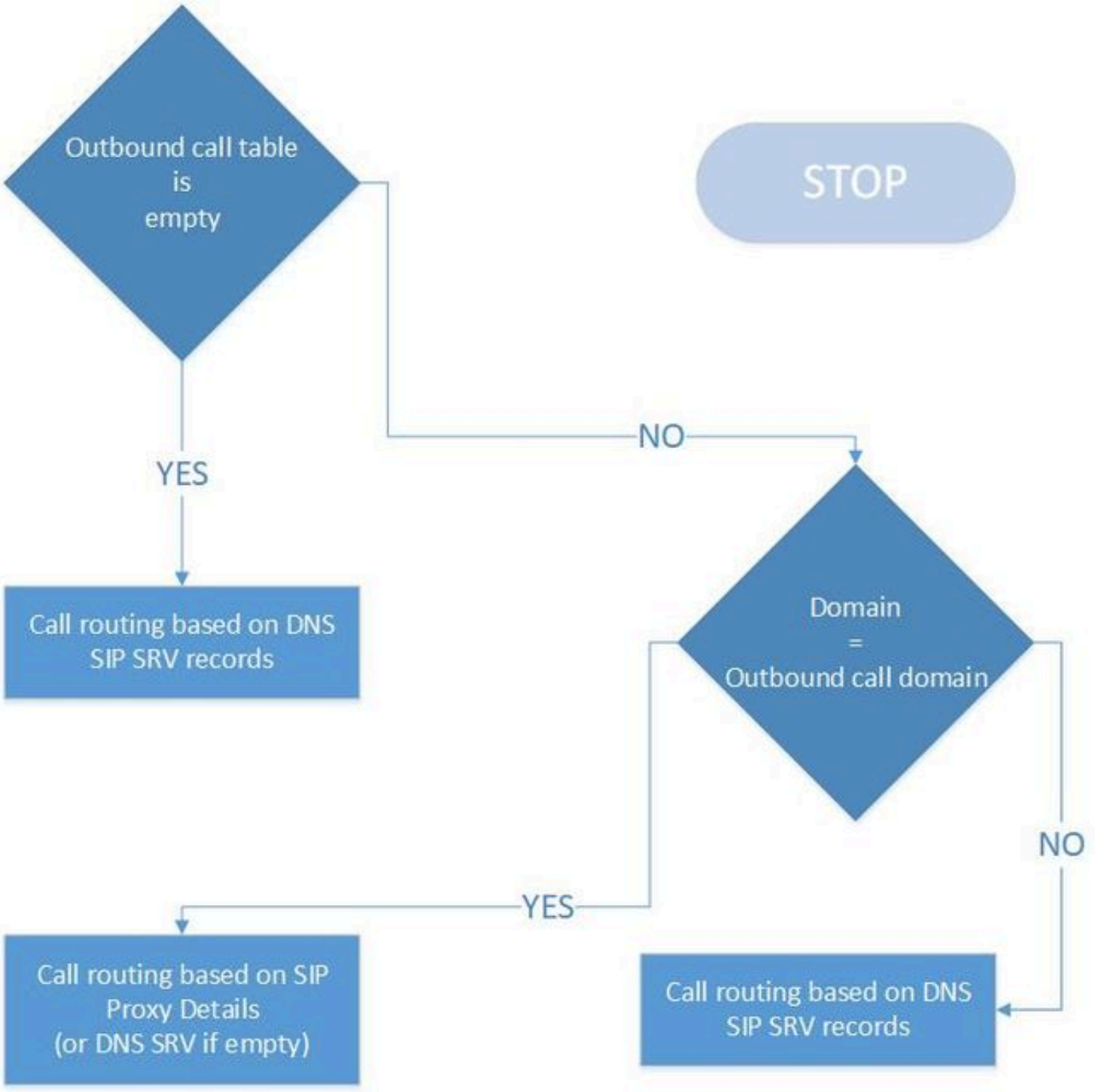
```
;transport=tcp>
2018-10-12  09:09:24.510  Info     SIP trace:

Ms-Conversation-ID

: 3P5Hu8grR1GGDF1BSMZAmw==
2018-10-12  09:09:24.510  Info     SIP trace: To: <sip:stejanss@newany.com>
2018-10-12  09:09:24.510  Info     SIP trace:

From

: "EX60 Steven" <sip:1060@

callbridgefqdn.any.com

>;tag=fb4ae780677e9d9b
```

如果轉發規則僅設定為pass through，則在From報頭上將不會出現任何修改，如上例所示（在這種情況下，轉發規則中設定pass through）。CMS啟動新的callLeg時，始終會調整聯絡人報頭，因此必須將聯絡人報頭增加到其自身中。

可以使用呼叫方ID、本地聯絡域和本地來自域的不同組合。出站SIP INVITE上的From報頭按照下表所示構建，入站呼叫在該表中使用usera@from.com的From報頭進入CMS。

Forwarding rule Caller ID	Outbound call rule Local contact domain	Outbound call rule Local from domain	Resulting from header
Pass through	NA	NA	usera@from.com
Use dial plan	NA	newfrom.com	usera@newfrom.com
Use dial plan	cms1.test.cms.com	<blank>	usera@cms1.test.cms.com
Use dial plan	<blank>	<blank>	usera@<ip_cms>

步驟 3.出站呼叫表



這是呼叫路由邏輯中將呼叫傳送到不同伺服器的最後一個表，如下所示：

- 傳入呼叫不在本地處理（在傳入呼叫匹配域上）。
- 它是來自CMS空間的出站呼叫(透過CMA或API，如果是TMS安排的會議，或者思科會議管理器(CMM)指示的出站呼叫)或來自CMA客戶端的出站呼叫。

從圖中可以看出邏輯是相對簡單的。如果表中完全沒有條目，它仍允許出站呼叫，但假設CMS伺服器能夠根據SIP請求URI上提及的特定域解析SIP SRV記錄(_sips._tcp / _sip._tcp / _sip._udp)。如果該表不是空的，但是撥號域沒有匹配項，則執行相同的DNS查詢邏輯。如果域中有匹配項，則遵循該特定規則的邏輯。在這方面，如果要阻止來自CMA的出站呼叫或透過TMS或CMM發出的出站呼叫，可以透過兩種方式執行此操作。沒有任何DNS SRV記錄（或無法由CMS解析），或者將這些呼叫路由到您的呼叫控制（例如CUCM或Expressway）並阻止那裡的呼叫。

下圖顯示了一個出站呼叫表示例：

Outbound calls

Filter Submit Query

■	Domain	SIP proxy to use	Local contact domain	Local from domain	Trunk type	Behavior	Priority	Encryption
□	steven.lab	<none; call directly>	contact.test.com	test.com	Standard SIP	Stop	5	Unencrypted
□	newany.com	10.48.36.46	callbridgefqdn.any.com	callbridgefqdn.any.com	Lync	Stop	4	Unencrypted
□	any.com	10.48.36.46		<use local contact domain>	Standard SIP	Stop	3	Unencrypted
□	test.cms.com	10.48.36.46		<use local contact domain>	Standard SIP	Stop	2	Unencrypted
□	vcs.steven.lab	10.48.36.46		<use local contact domain>	Standard SIP	Stop	1	Unencrypted
□	<match all domains>	10.48.36.215		<use local contact domain>	Standard SIP	Stop	0	Unencrypted
					Standard SIP	Stop	0	Auto

1

在末尾填入一般<匹配所有域>規則，在沒有填入SIP代理的情況下填入指向steven.lab域的第一個規則（因此它依賴於DNS SRV記錄）。

請注意，這是一個首先覆蓋的優先順序值較高的有序清單。如果匹配規則並且行為設定為「停止」，則在匹配之後呼叫不會透過表中的其餘部分，例如，如果SIP代理無法路由呼叫，則呼叫失敗。當該設定被設定為Continue時，您可以允許回退到集群中的其他路由或不同節點。例如，您可以為同一域的每個規則指定不同的SIP代理。

本地聯絡域和本地源域的設定將在傳入呼叫轉發表的上一節中介紹。中繼型別允許您指定需要撥打的呼叫型別，可以是標準SIP、Lync或Avaya（具體取決於接收系統）。

加密欄位確定呼叫的信令必須解密還是加密。但請注意，這並不意味著按照Configuration > Call Settings選單中的SIP媒體加密配置設定進行任何媒體加密。在此配置中，您還可選擇Auto（自動），嘗試首先使用加密信令進行呼叫，並可能回退到未加密信令。如果您事先知道另一端已加密或未加密，則強烈建議您對其進行相應定義，以避免由於回退進程導致的任何呼叫建立延遲。

在將DNS跟蹤和SIP跟蹤設定為詳細資訊的情況下，指向steven.lab的呼叫（在重寫傳入呼叫轉發表上的域之後）的日誌檔案的示例輸出向我們顯示了查詢的SRV記錄以及加密設定為自動時的回退機制。

<#root>

```
2018-10-12  11:25:16.168  Info      call 821: incoming SIP call from "sip:1060@steven.lab" to local URI
2018-10-12  11:25:16.179  Info      forwarding call to 'sip:stejanss@any.com' to 'stejanss@steven.lab'
2018-10-12  11:25:16.180  Info      call 822:
```

outgoing SIP call

```
 to "stejanss@
```

steven.lab

```
"

2018-10-12  11:25:16.180  Info      DNS trace: resolving "
```

steven.lab

```
" (SRV "
```

_sips._tcp

```
", dnsType:1) for call 822
2018-10-12  11:25:16.181  Info      DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for call 82
```

```
2018-10-12  11:25:16.181  Info     DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for call 82

succeeded

; results: 1
2018-10-12  11:25:16.181  Info     DNS trace: resolution of "steven.lab" (SRV "_sips._tcp") for call 82

10.48.36.215:5061

2018-10-12  11:25:16.181  Info     SIP trace: connection 45: allocated for outgoing encrypted connectio
2018-10-12  11:25:16.201  Info

handshake error

 336151576 on outgoing connection 45 to 10.48.36.215:5061 from 10.48.80.71:54864
2018-10-12  11:25:16.201  Info     SIP trace: connection 45: shutting down...

2018-10-12  11:25:16.201  Info     call 822:

falling back to unencrypted control connection

...

2018-10-12  11:25:16.201  Info     DNS trace: resolving "steven.lab" (SRV "

_sip._tcp

", dnsType:1) for call 822
2018-10-12  11:25:16.202  Info     DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for call 822
2018-10-12  11:25:16.202  Info     DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for call 822

succeeded

; results: 1
2018-10-12  11:25:16.202  Info     DNS trace: resolution of "steven.lab" (SRV "_sip._tcp") for call 822

10.48.36.215:5060

2018-10-12  11:25:16.202  Info     SIP trace: connection 46: allocated for outgoing connection to 10.48
2018-10-12  11:25:16.203  Info     SIP trace: connection 46: outgoing connection successful, 10.48.80.7
2018-10-12  11:25:16.205  Info     SIP trace: connection 46: outgoing SIP TCP data to 10.48.36.215:5060
2018-10-12  11:25:16.205  Info     SIP trace: INVITE sip:stejanss@steven.lab SIP/2.0
```

注意：如果是具有多個呼叫網橋的集群環境，您可以在透過API配置每個呼叫網橋並在該API對象上指定呼叫網橋ID（或callbridgeGroup ID）時設定每個呼叫網橋的出站撥號方案規則。例如，假設您希望所有呼叫都從某個特定域的特定Callbridge發出(例如，當您撥到us.example.com時，您希望它從您基於美國的伺服器發出)。然後確保您具有outboundDialPlanRules的API配置，以便基於美國的呼叫網橋以外的其他Callbridge能夠將呼叫路由到US Callbridge（在本例中）。

OutboundDialPlanRule(適用於US Callbridge)

- 域= us.example.com
- sipProxy = <使用DNS SRV/IP或FQDN時為空（如果手動設定）>
- 範圍= callbridge
- callbridge = <UScallbridge-ID>

OutboundDialPlanRules（適用於必須允許進行該呼叫的所有非美國Callbridge）（每個

Callbridge需要一個）

- 域= us.example.com
- sipProxy = <IP-or-FQDN-of-US-Callbridge>
- 範圍= callbridge
- callbridge = <non-US-callbridge-ID>

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

目前沒有適用於此組態的特定疑難排解資訊。

相關資訊

- 技術支援與文件 - Cisco Systems
- 合作解決方案分析器工具
- CMS檔案

註：有關配置示例，請參閱以下指南：

- 配置和整合CMS單一組合指南
- 《配置思科會議伺服器和CUCM指南》

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。